WHAT IS CLAIMED IS:

1. A method of performing a key exchange between a client and a server having a process-based security system comprising the steps of:

sending user identification information from the client to the server;

modifying the task structure of the client by the server to reflect a pending request for key exchange;

generating a first random number;

sending the first random number to the client;

retrieving a password associated with the user identification information by the server;

entering a password at the client;

calculating a first key using a transformative function operating on the password and the first random number by the server;

calculating a first key using the transformative function operating on password and the first random number by the client;

using the result of the calculated first key as a first key; and

modifying the task structure of the client by the server to reflect the completion of the key exchange.

2. The method of claim 1, wherein said client is a process executed on the server.

3. The method of claim 1, wherein said client is a process running on a remote machine.

4. The method of claim 1, wherein said transformative function is a hash function.

5. The method of claim 1, wherein said transformative function is a keyed MD5 signature function.

6. The method of claim 1, wherein said first key is used for communication using symmetric encryption.

7. The method of claim 1, wherein said first random number is generated using noise.

8. The method of claim 1, wherein said first random number number is sixteen bits in length.

9. The method of claim 1, further comprising the steps of:

generating a second random number by the server;

sending the second random number to the client;

calculating a second key using the transformative function operating on the password and second random number by the server;

calculating a second key using the transformative function operating on the password and second random number by the client;

using the calculated second key as a second key.

10. The method of claim 9, wherein said first key is used to encrypt communications from the client to the server and said second key is used to encrypt communications from the server to the client.

11. The method of claim 1, where said retrieved password is cleartext.

12. A system for key exchange between a client and key exchange server having a process-based security system comprising:

a key exchange server processor communicably connected to a client;

a key exchange server memory connected to said key exchange server processor;

wherein said key exchange server processor:

receives user identification information from said client;

modifies the task structure of the client to reflect a pending request for key exchange;

generates a first random number;

sends the first random number to the client;

retrieves a password associated with the user identification information from the key exchange server memory;

calculates a first key using a transformative function operating on the password and the first random number;

uses the result of the calculated first key as a first key; and

modifies the task structure of the client to reflect the completion of the key exchange.

13. The system of claim 12, wherein the key exchange server processor is communicably connected to the client by a network.

14. The system of claim 12, wherein said password is stored in said key exchange server memory as cleartext.

15. The system of claim 12, wherein the transformative function is a hash function.

16. The system of claim 12, wherein the transformative function is a keyed MD5 signature function.

17. The system of claim 12, wherein first key is used for symmetric encryption of communications between the client and the server.

18. The system of claim 12, wherein the key exchange server processor generates a second random number;

sends the second random number to the client;

calculates a second key using the transformative function operating on the password and second random number; and

uses the calculated second key as a second key.

19. The system of claim 18, wherein said first key is used to encrypt communications from the client to the server and said second key is used to encrypt communications from the server to the client.

20. The system of claim 18 wherein said second random number is generated using noise.